ABSTRACT

A random number generator includes a plurality of groups of independent flip flops, each of the groups having different configurations. Each of the outputs of the plurality of groups of flip flops being connected in an exclusive-or (XOR) arrangement, with a latch connected to the output of the DXOR. A metastable output of at least one of the flip flops causes a random signal to be output by the XOR for random number generation. The groups of flip flops can be divided into equally-sized groups, or unequally-sized groups with different configurations, such as the cross-connecting of NAND gates with or without buffers inserted between the data and clock signals, or inserting buffers between a data line of at least one NAND gate of each of the pairs of NAND gates being connected, or inserting a buffer between clock input of at least one NAND gate of each of the pairs of NAND gates being connected via a buffer. Capacitive loading and cross-connected buffers may also be used to induce varying delays.